CANDIDATE STANDARD

Mythos Documentation System Standard

Treat documentation as an engineered authority, evidence, traceability, and lifecycle system.

PERMANENT ID
MYTHOS-FND-0002

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Documentation System Standard

Universal Requirements for Documentation Authority, Architecture, Traceability, Evidence, Documentation-as-Code, and Lifecycle Governance

Document ID
MYTHOS-FND-0002

Version
1.0.0-candidate

Status
Candidate Standard

Review date
2027-09-17

Publication position
This is a permanent candidate standard in the Mythos Engineering Standards Library. Candidate status means the content is ready for structured implementation and review, but it is not represented as external certification, regulatory approval, or independent assurance.

PROFILE	CONTROLS	CADENCE	EVIDENCE
3 LEVELS	18	TRIGGERED	ASSESSABLE
Foundational / Advanced / High Assurance	Atomic normative controls	Annual plus material-change review	Examine / Interview / Test / Measure

Reader orientation

Dimension	Engineering position
Primary domain	Foundation and Governance
Audience	Technical writers and documentation engineers; Engineers and architects; Product, security, quality, and operations teams; AI and automation system designers; Auditors, assessors, and reviewers
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0002/

Expected outcomes

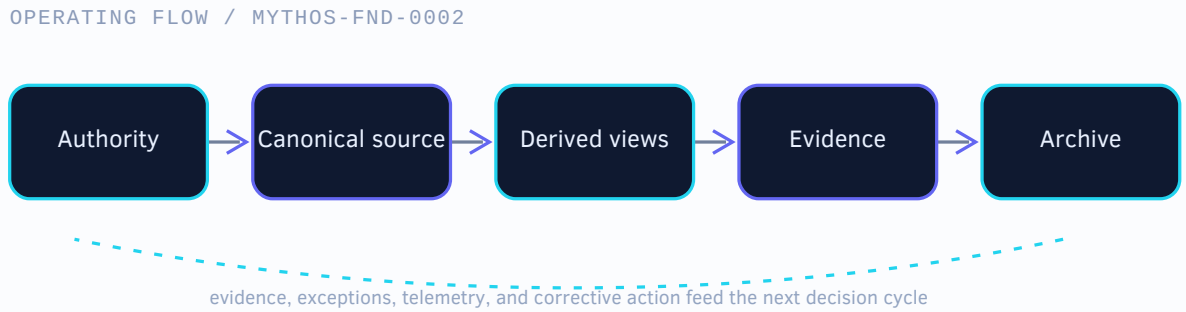
- Ensure every material claim has an identifiable authority, owner, status, and source.
- Make documentation discoverable and usable by engineers, operators, users, assessors, and authorized automation.
- Prevent stale plans, generated artifacts, and informal notes from silently overriding authoritative records.
- Integrate documentation quality and traceability into delivery and operations workflows.

SOURCE / FRESHNESS POSITION

Authority and source posture

Validated 2026-09-17
Primary authority versions were revalidated for this regeneration on 2026-09-17. Current-source updates are reflected where a newer stable version was identified; active drafts are labeled as such and do not silently replace current final authorities.

FOUNDATION OPERATING DOCTRINE



The source lineage for this edition is the enterprise candidate source set produced in July 2026. Normative controls are preserved; editorial, visual, metadata, and authority-freshness changes are recorded as revision lineage rather than presented as new control substance.

NAVIGATION

Contents

The table of contents is page-aware and internally linked. Control-level navigation follows on the next pages.

NORMATIVE SYSTEM

Control index

Every control is independently addressable and assessable. Page references link directly to the control record.

Document Control

Field	Value
Document ID	MYTHOS-FND-0002
Standard	Documentation System
Version	1.0.0-candidate
Status	Candidate Standard
Classification	Public
Publisher	Mythos Systems
Program	Mythos Engineering Standards Program
Accountable Owner	Mythos Systems Standards Program
Technical Review	Required
Source and Citation Review	Required
Assessment Review	Required
Accessibility and Publication Review	Required
Supersedes	No published edition; evolves source draft 0.2.0
Next Review	2027-09-17 or earlier on trigger

Revision Record

Version	Date	Status	Material Change
1.0.0-candidate	2026-09-17	Candidate Standard	Permanent-publication regeneration: source-preserving editorial system, richer information design, current authority revalidation, stable public metadata, and release QA.
0.2.0	2026-07-18	Working Draft	Source control standard
1.0.0-candidate	2026-07-22	Candidate Standard	Enterprise report architecture, executive direction, target operating model, profiles, maturity, authority register, and source-preserving reconstruction

How to Use This Standard

Executive Reading Path

Read Part I, the target-state architecture in Part III, the profile table in Part V, and the assurance dashboard in Part VI.

Engineering Reading Path

Read Parts II through V, then use the normative controls in Part IV as implementation and design requirements.

Assessment Reading Path

Read the conformance requirements in Part II, every applicable control's evidence and assessment procedure in Part IV, and the assessment, maturity, confidence, and traceability provisions in Parts VI and VII.

Normative and Informative Content

Uppercase **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** statements are normative when used under the requirements-language provisions of this document. Executive findings, examples, implementation patterns, reference architectures, mappings, and external-authority descriptions are informative unless explicitly incorporated into an adopting organization's binding policy, contract, or regulatory obligation.

FOUNDATION STANDARD / STRUCTURAL PART

Part I – Executive Direction

1. Executive Overview

Documentation is operational infrastructure. When teams cannot identify which document is authoritative, current, reviewed, applicable, and connected to implementation, engineering decisions become unrepeatable and operational risk rises. This standard defines documentation as a governed system of records, decisions, contracts, runbooks, evidence, and audience-specific guidance rather than a loose collection of files.

The institutional objective is to establish an authoritative, lifecycle-managed documentation system that makes products, systems, decisions, interfaces, operations, risks, tests, and user obligations understandable and traceable. Adoption should produce a controlled operating state in which leadership can understand the material risks, engineering teams can act on explicit requirements, assessors can test implementation and operating effectiveness, and the organization can support every conformance or trust claim with current evidence.

2. Executive Findings and Required Direction

Finding	Enterprise Exposure	Required Direction
Multiple competing truths	Wikis, tickets, repositories, and generated drafts often disagree without an authority model.	Publish a documentation map and canonical authority for every information class.
Stale but plausible guidance	Old documents remain discoverable and are mistaken for current direction.	Require status, supersession, review triggers, and drift detection.
Untraceable decisions	Architecture and product decisions are lost inside chats and meetings.	Capture decisions with rationale, alternatives, consequences, and supersession.
Generated-documentation risk	AI-generated text can create convincing but unsupported system descriptions.	Label generated content, require source pointers, and validate against observed implementation.
Unsafe machine consumption	Agents may ingest obsolete, malicious, or out-of-scope documents as instructions.	Separate source content from instructions and publish safe machine-consumption boundaries.

3. Business and Operational Impact

3.1 Strategic Impact

This standard converts a discipline that is often dependent on individual expertise into an organization-wide system of ownership, records, controls, review, and evidence. It reduces decision ambiguity and makes material assumptions visible before they become embedded in products or operations.

3.2 Delivery and Cost Impact

Adoption requires investment in accountable roles, authoritative records, validation, tooling, and review. That cost should be measured against avoidable rework, delayed releases, incidents, regulatory exposure, duplicated platforms, failed integrations, and unsupported product claims.

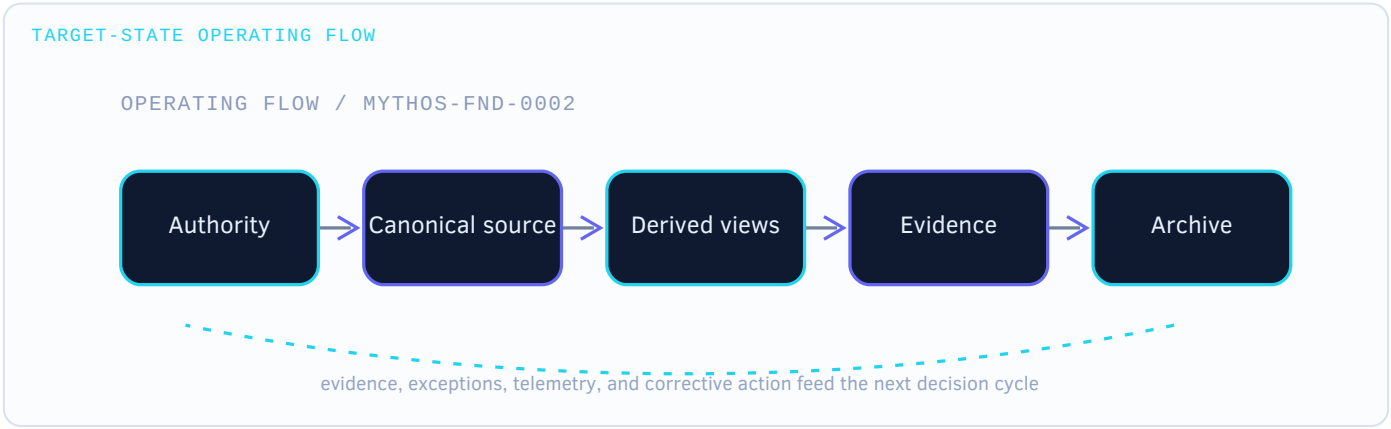
3.3 Security, Privacy, and Trust Impact

The standard requires security, privacy, integrity, resilience, and delegated authority to be considered within the primary operating model rather than as downstream approvals. This reduces the likelihood that unsafe boundaries become structurally expensive to correct.

3.4 Workforce and Organizational Impact

The organization must distinguish accountable ownership, implementation, approval, and independent challenge. Adoption may expose gaps in authority, skills, evidence, or cross-functional participation that require leadership action.

4. Target-State Summary



The target state contains the following institutional components:

#	Target-State Component
1	Documentation authority and ownership model
2	Canonical metadata and document identity
3	Authoritative documentation map
4	Risk-based documentation profiles
5	Status, review, supersession, and retirement lifecycle
6	Architecture and decision records
7	Contract and interface documentation
8	Traceability graph
9	Security, privacy, test, operations, release, and user information
10	Documentation-as-code pipeline
11	Generated-content governance
12	Machine and agent consumption boundary
13	Quality and drift management

```
Enterprise obligations and risk appetite
    ↓
Accountable ownership and governance
    ↓
Versioned policies, contracts, and authoritative records
    ↓
Engineering implementation and automated enforcement
    ↓
Operational telemetry, evidence, and exception handling
    ↓
Independent assessment and leadership review
    ↓
Corrective action, controlled change, and continuous improvement
```

5. Leadership Responsibilities

Role	Accountability
Executive sponsor	Requires documentation accountability for material systems.
Documentation owner	Owns the documentation system and publication policy.
Domain author	Maintains technically accurate content.
Architecture authority	Approves architecture and decision records.
Operations owner	Owns runbooks and operational procedures.
Security and privacy reviewer	Reviews sensitive and risk-bearing content.
Release manager	Ensures release documentation and evidence are complete.
Information architect	Maintains taxonomy, discoverability, templates, and audience paths.
Independent reviewer	Tests accuracy, completeness, currency, and traceability.

Leadership must ensure that exceptions are explicit, risk-owned, time-bounded, monitored, and retired. A maturity score or successful audit sample does not replace accountability for known nonconformance or residual risk.

FOUNDATION STANDARD / STRUCTURAL PART

Part II – Standard Foundation

6. Purpose and Objectives

- Ensure every material claim has an identifiable authority, owner, status, and source.
- Make documentation discoverable and usable by engineers, operators, users, assessors, and authorized automation.
- Prevent stale plans, generated artifacts, and informal notes from silently overriding authoritative records.
- Integrate documentation quality and traceability into delivery and operations workflows.

7. Scope

Applies to product, architecture, security, privacy, data, interface, contract, test, release, operations, user, governance, decision, and evidence documentation for systems of any implementation technology.

8. Intended Audience

- Technical writers and documentation engineers
- Engineers and architects
- Product, security, quality, and operations teams
- AI and automation system designers
- Auditors, assessors, and reviewers

9. Requirements Language and Conformance

The key words **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** are normative only when written in uppercase and are interpreted in accordance with RFC 2119 and RFC 8174.

A conformance claim MUST identify the assessed scope, standard version, selected assurance profile, tailoring decisions, evidence period, assessor, and unresolved findings. Profiles are cumulative unless a control explicitly states otherwise.

- **Foundational:** broadly applicable minimum controls.
- **Advanced:** stronger governance, automation, scale, and independent verification.
- **High Assurance:** continuous or independent validation, stronger isolation, adversarial testing, formal analysis, or cryptographic evidence where warranted.

10. Normative References from Source Draft

- **RFC 2119** — Key words for use in RFCs to Indicate Requirement Levels. https://www.rfc-editor.org/rfc/rfc2119

- **RFC 8174** — Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words. https://www.rfc-editor.org/rfc/rfc8174
- **MYTHOS-GOV-0001** — Mythos Engineering Standards Authoring and Benchmark Framework, Version 0.1.0. ../governance/01_MYTHOS_STANDARDS_AUTHORING_AND_BENCHMARK_FRAMEWORK.md

11. Informative References from Source Draft

- **ISO/IEC/IEEE 26514:2022** — Design and development of information for users. https://www.iso.org/standard/77451.html
- **ISO/IEC/IEEE 15288:2023** — Systems and software engineering — System life cycle processes. https://www.iso.org/standard/81702.html
- **ISO/IEC/IEEE 29148:2018** — Systems and software engineering — Life cycle processes — Requirements engineering. https://www.iso.org/standard/72089.html
- **NIST SP 800-218 v1.1** — Secure Software Development Framework (SSDF). https://csrc.nist.gov/pubs/sp/800/218/final
- **NIST SP 800-53 Rev. 5, Release 5.2.0** — Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

External mappings are informative unless explicitly incorporated into a contract or regulatory obligation. Adopted organizations remain responsible for validating current source versions and legal applicability.

12. Terms and Definitions

Term	Definition
Accountable owner	The person or formally delegated role that accepts responsibility for an outcome, decision, control, or risk.
Assessment object	The system, process, component, artifact, team, service, or organizational scope being evaluated.
Compensating control	An alternative safeguard that provides comparable risk reduction when the specified control cannot be implemented as written.
Conformance claim	A bounded statement that an identified scope satisfies the applicable requirements of a named standard version and assurance profile.
Evidence	Reviewable information that supports a conclusion about design, implementation, operation, or control effectiveness.
High Assurance	The cumulative profile requiring stronger independence, adversarial testing, continuous verification, or formal evidence where risk warrants it.
Residual risk	Risk remaining after controls, mitigations, and compensating measures are applied.
System	A product, service, application, platform, workflow, integration, operational capability, or combined socio-technical environment.
Tailoring	A documented decision to include, strengthen, parameterize, or mark a control not applicable based on scope and risk.
Authority class	A declared category indicating whether a document is policy, product authority, architecture authority, contract authority, decision authority, operational authority, evidence, or informational material.
Documentation map	The authoritative index describing what documents exist, their purpose, authority, status, owner, and recommended reading order.
Generated documentation	Documentation produced from code, schemas, configuration, telemetry, or another authoritative source through a reproducible process.
Documentation drift	A material divergence between documentation and the system, process, contract, or decision it claims to represent.

Term	Definition
Supersession	A controlled transition in which a document is replaced while historical identity and traceability are preserved.

13. Applicability and Tailoring

The organization MUST determine applicability at the control level. A not-applicable decision MUST identify the assessed scope, factual basis, approver, review date, and any assumptions that would invalidate the decision. Tailoring may strengthen or parameterize a control; it MUST NOT silently weaken a MUST requirement. Compensating controls require documented equivalence of risk reduction.

FOUNDATION STANDARD / STRUCTURAL PART

Part III – Risk and Architecture

14. Enterprise Problem and Risk Landscape

The principal enterprise risks addressed by this standard include inconsistent ownership, undocumented authority, uncontrolled change, local optimization, evidence gaps, stale assumptions, supplier dependence, false assurance, and the inability to determine whether the operating system still matches its approved intent.

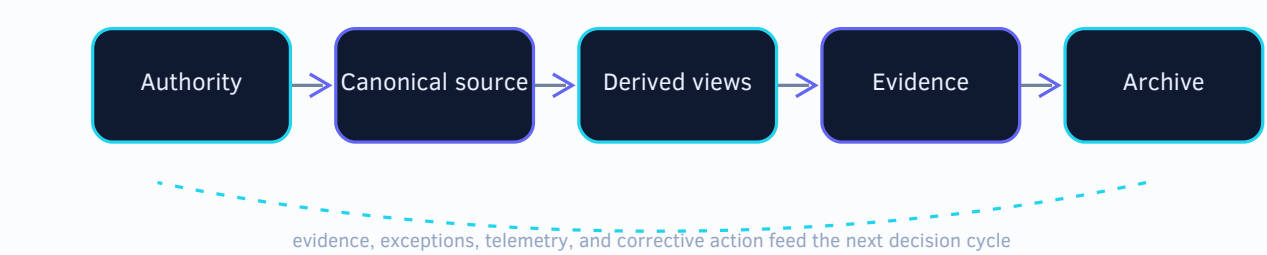
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected registers.

15. Governing Principles

- Documentation has explicit authority and conflict-resolution rules.
- The source of truth is named; generated views do not silently become authorities.
- Documentation is versioned, reviewable, testable, and maintained with the system.
- Current state, future intent, evidence, and historical record remain distinguishable.
- Documentation must support both human judgment and safe machine retrieval.
- Operational documents are validated through use, not merely publication.

16. Reference Operating Architecture

REFERENCE OPERATING ARCHITECTURE



```
Enterprise obligations and risk appetite
    ↓
Accountable ownership and governance
    ↓
Versioned policies, contracts, and authoritative records
    ↓
Engineering implementation and automated enforcement
    ↓
Operational telemetry, evidence, and exception handling
    ↓
Independent assessment and leadership review
    ↓
Corrective action, controlled change, and continuous improvement
```

16.1 Control Plane

The control plane contains accountable ownership, policy, standards, risk decisions, approvals, exception governance, and authoritative state. It MUST be distinguishable from implementation and reporting systems.

16.2 Delivery and Enforcement Plane

The delivery plane contains engineering workflows, automation, validation, configuration, runtime enforcement, and lifecycle processes. Automated enforcement SHOULD be preferred where requirements can be expressed and tested safely.

16.3 Evidence and Assurance Plane

The assurance plane collects evidence, observations, test results, decisions, exceptions, and historical state. Evidence systems MUST protect integrity, scope, provenance, retention, and authorized access.

16.4 Feedback Plane

Metrics, incidents, assessments, user outcomes, exceptions, and changing authorities feed corrective action and controlled revision. Feedback MUST not silently alter normative requirements or accepted risk.

17. Roles and Accountability

Role	Accountability
Executive sponsor	Requires documentation accountability for material systems.
Documentation owner	Owns the documentation system and publication policy.
Domain author	Maintains technically accurate content.
Architecture authority	Approves architecture and decision records.
Operations owner	Owns runbooks and operational procedures.
Security and privacy reviewer	Reviews sensitive and risk-bearing content.
Release manager	Ensures release documentation and evidence are complete.
Information architect	Maintains taxonomy, discoverability, templates, and audience paths.
Independent reviewer	Tests accuracy, completeness, currency, and traceability.

18. State, Evidence, and Decision Model

The adopting organization MUST distinguish:

- approved intent;
- current implemented state;
- observed operational state;
- generated or inferred recommendations;
- accepted exceptions;
- historical state;
- independently verified results.

A generated report, model conclusion, roadmap, or design proposal MUST NOT be represented as implemented or verified state without supporting evidence.

19. Security and Trust Considerations

Every implementation of this standard MUST apply identity, authorization, classification, least privilege, evidence integrity, sensitive-data handling, and supplier-risk controls appropriate to impact. Machine-generated guidance, automation, extensions, and delegated agents MUST remain subject to external policy and independent verification.

20. Failure Modes

Failure or Anti-Pattern	Enterprise Consequence
Treating chat transcripts as authoritative documentation	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Maintaining duplicate current documents without precedence	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Publishing generated text without provenance or review	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Runbooks that describe goals but not executable steps	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Architecture diagrams without version or scope	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Deleting superseded decisions instead of preserving history	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

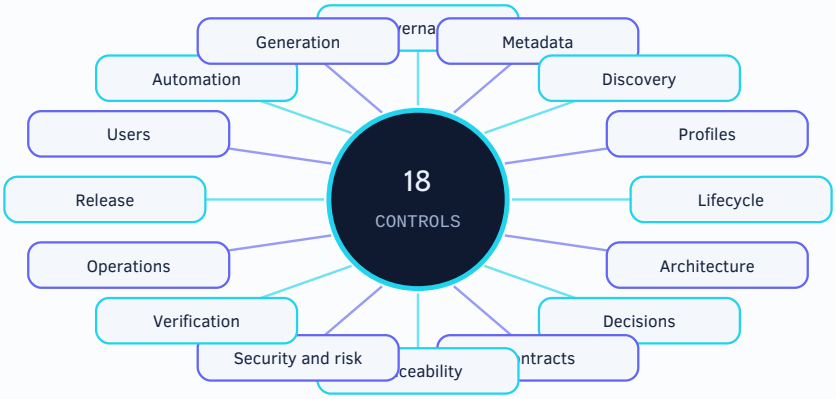
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter applicable control or a documented authority decision.

FOUNDATION STANDARD / STRUCTURAL PART

Part IV – Normative Control System

22. Control-Family Overview

CONTROL-FAMILY CONSTELLATION



This standard contains **18 controls** across the following families:

- Governance
- Metadata
- Discovery
- Profiles
- Lifecycle
- Architecture
- Decisions
- Contracts
- Traceability
- Security and risk
- Verification
- Operations
- Release
- Users
- Automation
- Generation
- Machine consumption
- Quality

23. Normative Controls

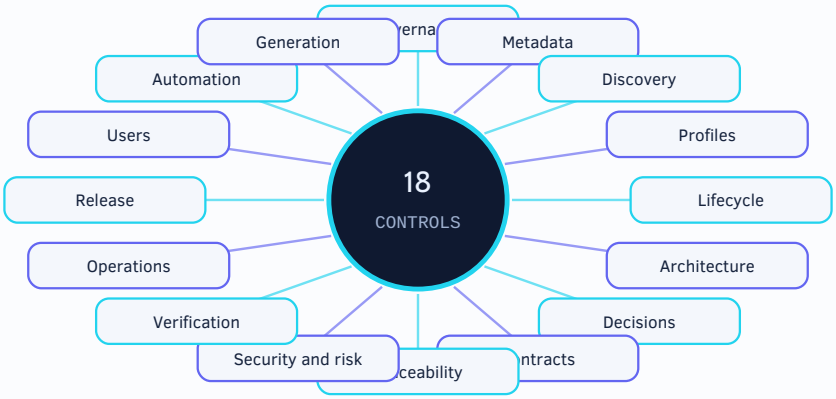
CONTROL SET
18
atomic requirements

PROFILES
3
cumulative assurance levels

ASSESSMENT
4
Examine / Interview / Test / Measure

Each control is independently addressable, evidence-bound, and assessable. The following control records preserve the source requirements while presenting implementation guidance, required evidence, assessment procedures, exceptions, compensating controls, and external mappings as a consistent engineering system.

NORMATIVE CONTROL CONSTELLATION



NORMATIVE CONTROL

MYTHOS-FND-DOC-01 – Documentation authority model

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Governance	Foundational, Advanced, High Assurance	Critical	Partial

Requirement

The organization MUST define documentation authority classes and an explicit conflict-resolution order that identifies which artifact governs when statements disagree.

Purpose

Prevents informal notes, stale plans, generated files, or presentation material from overriding policy, contracts, decisions, or current-state authority.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Define at minimum policy, product, architecture, contract, decision, operational, evidence, and informational classes.
- Declare the authority class in metadata.
- Require conflicts to be resolved rather than silently interpreted.

Required evidence

- Authority policy
- Sample metadata
- Conflict resolution records

Assessment procedure

- **Examine:** Examine whether authority classes are consistently used.
- **Interview:** Present a conflict scenario and verify the resolution path.
- **Test:** Sample resolved conflicts for traceability.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 15288:2023 — information management

NORMATIVE CONTROL

MYTHOS-FND-DOC-02 – Canonical metadata and identity

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Metadata	Foundational, Advanced, High Assurance	Material	High

Requirement

Authoritative documents MUST have a stable identifier, title, version, status, owner, approver or approval authority, classification, effective date, review trigger or interval, and supersession relationship where applicable.

Purpose

Enables reliable discovery, governance, lifecycle management, citation, and machine processing.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Use repository-independent IDs.
- Separate content version from file path or storage revision.
- Validate required metadata automatically.

Required evidence

- Metadata schema
- Validation results
- Sample document headers

Assessment procedure

- **Examine:** Examine metadata completeness and uniqueness.
- **Interview:** Test automated rejection of missing required fields.
- **Test:** Verify moved or renamed documents retain stable identity.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 26514:2022 — information management

NORMATIVE CONTROL

MYTHOS-FND-DOC-03 – Authoritative documentation map

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Discovery	Foundational, Advanced, High Assurance	Material	High

Requirement

Each product, service, or governed program MUST maintain a documentation map that identifies authoritative documents, owners, statuses, audiences, known gaps, historical material, and recommended reading paths.

Purpose

Reduces search cost and prevents users or automated systems from relying on the first discoverable but non-authoritative artifact.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Provide role-based reading paths for new engineers, operators, security reviewers, product owners, and machine consumers.
- Link superseded content through history rather than mixing it with active guidance.
- Treat missing required documents as visible gaps.

Required evidence

- Documentation map
- User retrieval test results
- Gap register

Assessment procedure

- **Examine:** Ask representative users to locate authoritative answers.
- **Interview:** Verify every listed artifact exists and metadata agrees.
- **Test:** Sample repository documents not in the map and determine disposition.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 26514:2022 — information architecture

NORMATIVE CONTROL

MYTHOS-FND-DOC-04 – Risk-based documentation profile

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Profiles	Foundational, Advanced, High Assurance	Material	Partial

Requirement

The organization MUST select and document a documentation profile proportionate to system complexity, lifecycle, user impact, regulatory exposure, operational criticality, data sensitivity, and extension or AI capabilities.

Purpose

Avoids both under-documentation of high-risk systems and wasteful documentation requirements for low-risk utilities.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Define minimum required artifact classes per profile.
- Allow lean documents to combine concerns when authority and ownership remain clear.
- Strengthen documentation following incidents, scale increases, new integrations, or material autonomy.

Required evidence

- Selected profile
- Tailoring rationale
- Required-document checklist

Assessment procedure

- **Examine:** Examine whether the profile matches risk.
- **Interview:** Verify required classes are present or explicitly tailored.
- **Test:** Review profile changes after material triggers.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-53 Rev. 5 — PL family

NORMATIVE CONTROL

MYTHOS-FND-DOC-05 – Status, review, and supersession lifecycle

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Lifecycle	Foundational, Advanced, High Assurance	Critical	High

Requirement

Authoritative documents MUST use a controlled lifecycle with defined status meanings, promotion criteria, review triggers, deprecation rules, supersession links, and historical retention.

Purpose

Prevents draft or obsolete material from being treated as approved and preserves decision history without creating ambiguity.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Use statuses such as working draft, reviewed draft, approved, deprecated, superseded, and withdrawn.
- Display prominent notices on non-current documents.
- Trigger review after relevant incidents, architecture changes, interface changes, or source-standard updates.

Required evidence

- Lifecycle policy
- Review and approval records
- Supersession graph

Assessment procedure

- **Examine:** Examine status consistency.
- **Interview:** Test links from superseded to successor documents.
- **Test:** Sample overdue reviews and verify escalation.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 15288:2023 — configuration management

NORMATIVE CONTROL

MYTHOS-FND-DOC-06 – Architecture documentation and invariants

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Architecture	Foundational, Advanced, High Assurance	Critical	Partial

Requirement

Architecture documentation MUST describe system context, components, responsibilities, data and control flows, trust boundaries, deployment variants, dependencies, failure domains, and invariants at a level sufficient for implementation and independent review.

Purpose

Makes architecture decisions and risk-bearing boundaries visible rather than implicit in code or tribal knowledge.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Use multiple views when one diagram cannot represent logical, deployment, data, security, and operational concerns.
- Record assumptions and known omissions.
- Keep diagrams as text or reproducible source where practical.

Required evidence

- Architecture description
- Diagrams and source
- Invariant register

Assessment procedure

- **Examine:** Trace a critical workflow through documented components.
- **Interview:** Compare deployed topology with architecture claims.
- **Test:** Interview maintainers about undocumented boundaries.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 15288:2023 — architecture definition

NORMATIVE CONTROL

MYTHOS-FND-DOC-07 – Architecture and product decision records

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Decisions	Foundational, Advanced, High Assurance	Material	Partial

Requirement

Material decisions MUST be recorded with context, decision, alternatives, consequences, risks, validation, owner, date, and revisit triggers; accepted decision records MUST remain immutable except for metadata and supersession links.

Purpose

Preserves rationale, supports future reversal, and prevents recurring debates or undocumented architecture drift.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Define triggers such as new dependencies, irreversible data models, trust-boundary changes, public contracts, and significant cost commitments.
- Create a new superseding record rather than rewriting history.
- Link decisions to requirements and implementation.

Required evidence

- Decision records
- Supersession links
- Validation evidence

Assessment procedure

- **Examine:** Sample changes and determine whether decisions were recorded.
- **Interview:** Verify alternatives and negative consequences are substantive.
- **Test:** Trace a superseded decision to current authority.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 15288:2023 — decision management

NORMATIVE CONTROL

MYTHOS-FND-DOC-08 – Contract and interface documentation

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Contracts	Foundational, Advanced, High Assurance	Critical	High

Requirement

Externally or internally consumed interfaces, schemas, events, configuration formats, extension contracts, and command behaviors MUST have versioned, machine-readable contracts or precise normative documentation with compatibility rules.

Purpose

Reduces integration ambiguity and enables automated validation of compatibility and behavior.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Name the authoritative source for each contract.
- Generate human-readable views from machine-readable contracts where feasible.
- Document errors, limits, authorization, deprecation, and examples.

Required evidence

- API or schema specifications
- Compatibility policy
- Contract test results

Assessment procedure

- **Examine:** Validate examples against the contract.
- **Interview:** Test backward-compatibility claims.
- **Test:** Verify documentation and implementation derive from the same authority.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- OpenAPI Specification 3.2.0
- JSON Schema 2020-12

NORMATIVE CONTROL

MYTHOS-FND-DOC-09 – Documentation traceability graph

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Traceability	Advanced, High Assurance	Critical	High

Requirement

The documentation system MUST support bidirectional traceability among source obligations, requirements, risks, decisions, architecture, contracts, implementation, tests, evidence, releases, incidents, and lifecycle status for material items.

Purpose

Allows impact analysis, completeness assessment, and reliable explanation of why the system exists and how it is verified.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Use stable identifiers rather than fragile heading links.
- Record relationship type and rationale.
- Detect orphaned and stale relationships automatically where practical.

Required evidence

- Traceability graph or matrix
- Coverage report
- Sample traces

Assessment procedure

- **Examine:** Trace selected obligations end to end.
- **Interview:** Modify a requirement in a test environment and verify affected artifacts are identified.
- **Test:** Review unexplained orphan nodes.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 29148:2018 — traceability

NORMATIVE CONTROL

MYTHOS-FND-DOC-10 – Security, privacy, and risk documentation

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Security and risk	Foundational, Advanced, High Assurance	Critical	Partial

Requirement

Systems handling material risk MUST maintain current security architecture, threat and abuse models, data classifications, authorization rules, privacy assessments, exception records, incident procedures, and risk ownership appropriate to scope.

Purpose

Ensures security and privacy decisions are reviewable, operationally usable, and connected to implementation.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Avoid duplicating secrets or sensitive exploitation details in broadly accessible documentation.
- Classify and access-control sensitive artifacts.
- Link mitigations to controls and tests.

Required evidence

- Security and privacy document set
- Access controls
- Threat-to-test traceability

Assessment procedure

- **Examine:** Examine completeness against risk.
- **Interview:** Verify sensitive documentation access.
- **Test:** Trace sampled threats to implementation and validation.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-53 Rev. 5 — PL, RA, CA families

NORMATIVE CONTROL

MYTHOS-FND-DOC-11 – Test strategy and evidence documentation

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Verification	Foundational, Advanced, High Assurance	Critical	High

Requirement

The organization MUST document verification and validation strategy, test scope, environments, data, expected results, limitations, evidence provenance, and disposition of failures for release-relevant requirements.

Purpose

Prevents pass claims without reproducible context and distinguishes planned testing from executed evidence.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Separate test design from execution evidence.
- Preserve tool versions, configuration, timestamps, and artifact hashes for high-impact evidence.
- Document known blind spots and nondeterminism.

Required evidence

- Test strategy
- Test catalog
- Evidence bundles and failure records

Assessment procedure

- **Examine:** Reproduce a sampled test from documentation.
- **Interview:** Verify failed results cannot be overwritten without history.
- **Test:** Compare release claims with evidence.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-53A Rev. 5 — assessment evidence

NORMATIVE CONTROL

MYTHOS-FND-DOC-12 – Actionable runbooks and operational documentation

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Operations	Foundational, Advanced, High Assurance	Critical	Partial

Requirement

Critical operational procedures MUST document trigger, preconditions, safety warnings, detection, diagnosis, action, verification, rollback or recovery, escalation, evidence preservation, and last exercise date.

Purpose

Makes operations repeatable under stress and reduces dependence on individual memory.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Write steps around observable conditions rather than assumed causes.
- Include permissions and blast-radius warnings.
- Exercise high-impact runbooks through simulation, game day, or live use at defined intervals.

Required evidence

- Runbooks
- Exercise records
- Post-use improvements

Assessment procedure

- **Examine:** Observe an operator use a sampled runbook.
- **Interview:** Verify rollback and escalation paths.
- **Test:** Review stale or never-exercised procedures.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-61 Rev. 3 — incident response documentation

NORMATIVE CONTROL

MYTHOS-FND-DOC-13 – Release documentation and evidence manifest

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Release	Foundational, Advanced, High Assurance	Critical	High

Requirement

Each governed release MUST include release notes, known limitations, compatibility and migration information, security and quality status, deployment and rollback instructions, evidence references, and an immutable manifest of released artifacts.

Purpose

Supports safe adoption, reproducibility, support, audit, and rollback.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Distinguish user-visible changes from internal changes.
- Identify deprecated and removed behavior.
- Hash or sign evidence and artifacts for higher-assurance releases.

Required evidence

- Release notes
- Release manifest
- Artifact and evidence hashes

Assessment procedure

- **Examine:** Verify a deployed artifact matches the manifest.
- **Interview:** Trace a release statement to evidence.
- **Test:** Test rollback instructions in a representative environment.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SSDF v1.1 — produce well-secured releases

NORMATIVE CONTROL

MYTHOS-FND-DOC-14 – Audience-appropriate user information

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Users	Foundational, Advanced, High Assurance	Material	Manual

Requirement

User, administrator, operator, developer, and support documentation MUST address the tasks, permissions, risks, failure modes, and recovery needs of each applicable audience without assuming internal implementation knowledge.

Purpose

Reduces misuse, unsafe operation, support burden, and exclusion caused by documentation written only for builders.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Use task-oriented structure.
- Clearly distinguish warnings, prerequisites, expected results, and troubleshooting.
- Evaluate accessibility, localization, and reading context.

Required evidence

- Audience map
- Published user information
- Usability and retrieval test results

Assessment procedure

- **Examine:** Ask representative users to complete tasks using documentation.
- **Interview:** Review support cases for documentation gaps.
- **Test:** Verify inaccessible or privileged steps are labeled.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 26514:2022 — information for users

NORMATIVE CONTROL

MYTHOS-FND-DOC-15 – Documentation-as-code controls

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Automation	Foundational, Advanced, High Assurance	Material	High

Requirement

Documentation stored with or governing software and infrastructure SHOULD be version-controlled, reviewed, linted, link-checked, rendered reproducibly, and validated in delivery workflows before merge or release.

Purpose

Applies engineering controls to documentation and catches structural defects before publication.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Validate metadata, identifiers, terminology, references, links, schemas, and generated outputs.
- Use protected branches or equivalent review controls for authoritative documents.
- Keep build tooling and dependencies pinned where reproducibility matters.

Required evidence

- Repository history
- CI results
- Publication build manifest

Assessment procedure

- **Examine:** Introduce a controlled documentation error and verify detection.
- **Interview:** Review bypass privileges.
- **Test:** Reproduce a published artifact from source.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SSDF v1.1 — protect software and development artifacts

NORMATIVE CONTROL

MYTHOS-FND-DOC-16 – Generated-documentation boundaries

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Generation	Foundational, Advanced, High Assurance	Material	High

Requirement

Generated documentation MUST identify its authoritative source, generation method, timestamp or version, and overwrite policy; generated output MUST NOT be manually edited when regeneration would discard or conceal the change.

Purpose

Prevents divergence between code or schema authority and human-modified generated copies.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Mark generated files prominently.
- Fail generation when source and output are inconsistent if output is committed.
- Place authored commentary in supported extension points.

Required evidence

- Generator configuration
- Generated-file headers
- Drift check results

Assessment procedure

- **Examine:** Modify generated output and verify drift detection.
- **Interview:** Trace a generated claim to source.
- **Test:** Confirm manual extension points survive regeneration.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 26514:2022 — information development

NORMATIVE CONTROL

MYTHOS-FND-DOC-17 – Safe machine and AI consumption

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Machine consumption	Advanced, High Assurance	Critical	High

Requirement

Documentation supplied to search, retrieval, automation, or AI systems MUST preserve authority, status, provenance, access controls, supersession, and citation metadata, and MUST prevent unauthorized material from being promoted as trusted context.

Purpose

Reduces hallucination, stale guidance, data leakage, and automation based on non-authoritative content.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Index document sections with stable IDs and source metadata.
- Apply access control before retrieval, not only after generation.
- Prefer authoritative current material and expose uncertainty or conflicts.
- Evaluate retrieval and citation quality with representative tasks.

Required evidence

- Ingestion policy
- Retrieval test corpus
- Access-control and citation results

Assessment procedure

- **Examine:** Query known conflicting or superseded material.
- **Interview:** Test unauthorized retrieval attempts.
- **Test:** Measure whether generated answers cite the correct current authority.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST AI RMF 1.0 — Map and Measure
- NIST AI 600-1 — content provenance and information integrity

NORMATIVE CONTROL

MYTHOS-FND-DOC-18 – Documentation quality and drift management

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Quality	Foundational, Advanced, High Assurance	Critical	High

Requirement

The organization MUST monitor material documentation defects, unresolved gaps, broken references, stale ownership, retrieval failures, and documented-versus-actual drift, with severity, ownership, remediation targets, and escalation.

Purpose

Turns documentation quality into an observable operational concern rather than an occasional cleanup activity.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Prioritize defects that could cause unsafe actions, invalid compliance claims, or failed recovery.
- Use production incidents and support trends as documentation signals.
- Publish known gaps rather than concealing them.

Required evidence

- Documentation quality dashboard
- Defect and gap register
- Drift remediation records

Assessment procedure

- **Examine:** Review aging and severity trends.
- **Interview:** Sample closed defects for verified correction.
- **Test:** Compare selected documentation claims to live system evidence.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 26514:2022 — quality management

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Canonical metadata, owner, status, authoritative map, essential architecture, interface, runbook, release, and user documentation.
Enterprise	Documentation-as-code, automated link and freshness checks, traceability graph, generated-content controls, audience portals, and review dashboards.
High Assurance	Independent source validation, signed release documentation, protected evidence, controlled machine corpus, formal document baselines, and continuous drift detection.

Profiles are cumulative unless a control explicitly states otherwise. A higher profile cannot be claimed solely through additional tooling; governance, evidence, operating effectiveness, and independent challenge must also satisfy the profile.

25. Implementation Lifecycle

25.1 Establish

- appoint accountable ownership;
- determine applicability and profile;
- inventory current processes, systems, records, and known exceptions;
- identify authority sources and legal applicability;
- establish evidence locations and review cadence.

25.2 Baseline

- assess every applicable control;
- distinguish implemented, partially implemented, not implemented, not applicable, and not assessed;
- record evidence quality and confidence;
- identify systemic dependencies and priority risks.

25.3 Implement

- define target architecture and ownership;
- create or revise policies, contracts, workflows, and controls;
- automate enforcement and evidence where safe;
- test failure and recovery paths;
- train accountable roles.

25.4 Assure

- conduct technical and procedural assessment;
- verify evidence over a representative period;
- test sampled controls and critical workflows;
- challenge exceptions, unsupported claims, and optimistic assumptions.

25.5 Operate and Improve

- monitor metrics and exceptions;
- investigate incidents and control failures;
- update for authority, threat, technology, or organizational change;
- preserve superseded decisions and evidence;
- retire obsolete controls and implementations deliberately.

26. Integration Requirements

Implementations SHOULD integrate the standard with product governance, architecture review, secure development, CI/CD, change management, observability, service management, identity, evidence, risk, procurement, and training systems. Integration MUST preserve ownership and source authority rather than copying uncontrolled state between tools.

27. Failure Handling and Recovery

Control failures MUST produce a classified finding, owner, containment or compensating action, due date, evidence requirement, and escalation path. Where failure creates ongoing material risk, the organization MUST consider stopping, restricting, rolling back, isolating, or retiring the affected activity.

28. Exceptions and Compensating Controls

Exceptions MUST identify the exact control, scope, rationale, risk, owner, approval, compensating measures, monitoring, expiration, and closure evidence. Exceptions MUST NOT be used to convert a permanent design weakness into nominal conformance.

29. Prohibited Practices

- Treating chat transcripts as authoritative documentation
- Maintaining duplicate current documents without precedence
- Publishing generated text without provenance or review
- Runbooks that describe goals but not executable steps
- Architecture diagrams without version or scope
- Deleting superseded decisions instead of preserving history

30. Adoption Roadmap from Source Draft

- Define the authority model, metadata schema, repository structure, and documentation map.

- Establish required documentation profiles and stable identifiers for requirements, decisions, contracts, tests, and runbooks.
- Add documentation-as-code checks, link validation, ownership enforcement, and lifecycle statuses.
- Implement traceability, generated-document boundaries, release evidence, and runbook exercises.
- For Advanced and High Assurance adoption, add structured schemas, signed evidence, retrieval evaluation, and continuous drift detection.

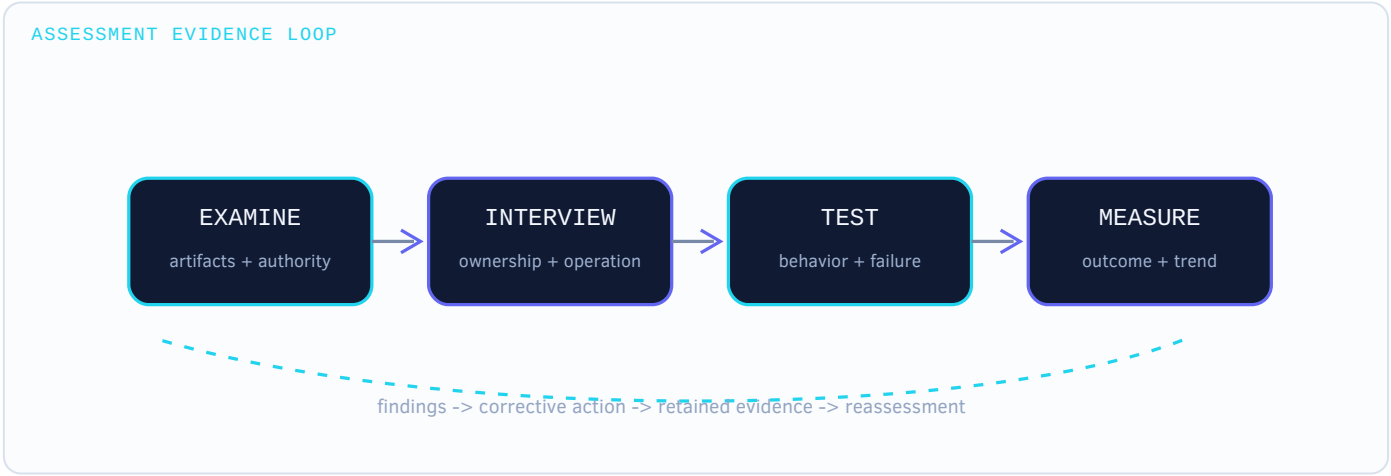
31. Limitations and Residual Risk from Source Draft

Conformance demonstrates that defined requirements were satisfied within a bounded scope and evidence period. It does not guarantee absence of defects, compromise, harm, outage, legal exposure, or future failure. Novel threats, misunderstood dependencies, invalid assumptions, human error, supplier changes, and conditions outside the assessment scope remain possible.

FOUNDATION STANDARD / STRUCTURAL PART

Part VI – Assurance and Assessment

32. Assessment Methodology



Assessors MUST use a combination of examination, interview, and testing appropriate to the selected profile and control risk. Assessment records MUST identify sample size, tools, versions, evidence references, exclusions, limitations, confidence, and residual uncertainty. Automated checks MAY support a finding but MUST NOT be treated as proof of effective governance or operation when the control depends on human accountability or contextual judgment.

12.1 Finding States

- **Satisfied:** requirement implemented and supported by sufficient evidence.
- **Partially satisfied:** some required outcomes or scope are missing.
- **Not satisfied:** requirement absent, ineffective, or contradicted by evidence.
- **Not applicable:** supported by an approved tailoring rationale.
- **Not assessed:** evidence is insufficient.

12.2 Conformance

A scope is **Conformant** only when all applicable MUST controls for the claimed profile are satisfied. A failed critical MUST control cannot be averaged away by stronger performance elsewhere.

33. Metrics and Reporting from Source Draft

Metric	Definition	Expected use or target
Authoritative-document coverage	Required document classes with current approved owners and status	100% for selected profile
Broken trace links		0 critical; declining total

Metric	Definition	Expected use or target
	Invalid or unresolved references among requirements, decisions, contracts, tests, and releases	
Documentation drift age	Time between material system change and authoritative documentation reconciliation	Defined per risk; continuous or release-bound for High Assurance
Runbook exercise rate	Critical runbooks exercised within their required interval	100%
Retrieval success	Representative users able to locate the authoritative answer without escalation	>= 90% in sampled tasks

Metrics MUST be interpreted with scope and uncertainty. Organizations SHOULD report trends, distributions, and exceptions rather than presenting a single composite score as complete assurance.

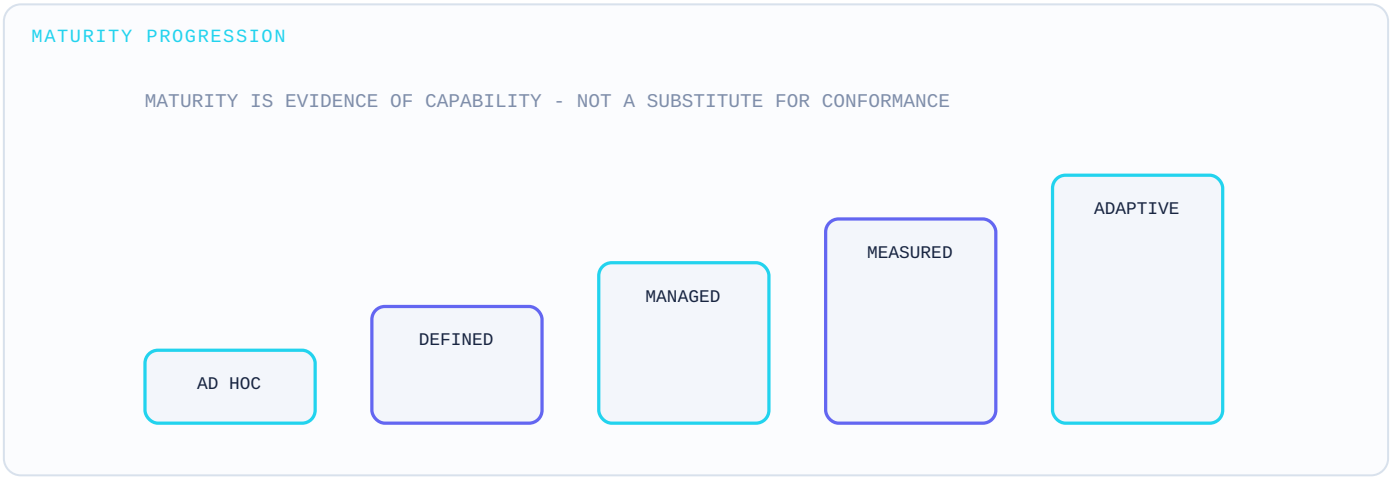
34. Exceptions and Compensating Controls

Every exception MUST identify the affected control and scope, justification, risk, compensating controls, accountable approver, start and expiration dates, monitoring, and remediation or retirement plan. Exceptions MUST be reevaluated after material change or incident and MUST NOT be self-approved by the team or agent requesting the exception where separation of duties is required.

35. Enterprise Metric Set

Metric	Measurement Requirement
documents with current owner and review date	Defined by the adopting organization with owner, source, target, and cadence.
authoritative information classes with one designated source	Defined by the adopting organization with owner, source, target, and cadence.
broken references	Defined by the adopting organization with owner, source, target, and cadence.
superseded documents still presented as current	Defined by the adopting organization with owner, source, target, and cadence.
documented decisions linked to implementation	Defined by the adopting organization with owner, source, target, and cadence.
runbooks validated through exercise	Defined by the adopting organization with owner, source, target, and cadence.
generated claims without source pointers	Defined by the adopting organization with owner, source, target, and cadence.
documentation drift findings unresolved beyond target	Defined by the adopting organization with owner, source, target, and cadence.

36. Maturity Model



Level	Name	Required Characteristics
M0	Unmanaged	Outcome is not intentionally controlled or evidence is unavailable.
M1	Documented	Ownership and procedures exist but implementation is inconsistent or mostly manual.
M2	Implemented	Applicable controls operate in the assessed scope and evidence exists.
M3	Measured	Effectiveness, exceptions, failures, and trends are measured and reviewed.
M4	Assured	Independent testing, representative evidence, and continuous or periodic validation exist.
M5	Adaptive	Controls respond safely to changing risk, authority, technology, and operational evidence.

Maturity does not override conformance. An organization cannot compensate for a failed mandatory requirement by assigning itself a high maturity level.

37. Assessment Confidence

Assessment confidence MUST be recorded as Low, Moderate, High, or Very High. Confidence considers evidence integrity, observation period, sample coverage, source authority, environmental representativeness, test repeatability, reviewer independence, and unresolved gaps.

38. Executive Assurance Dashboard

The executive report SHOULD present:

- applicable controls;
- conformant, partial, nonconformant, exception, not applicable, and not assessed counts;
- high and critical findings;
- evidence freshness;
- exception age;
- maturity distribution;
- assessment confidence;
- top residual risks;

- corrective-action status.

FOUNDATION STANDARD / STRUCTURAL PART

Part VII – Authority and Traceability

39. Cross-Standard Dependencies from Source Draft

This standard is part of an integrated foundation. Product decisions depend on documentation and traceability; implementation depends on security, quality, data, interfaces, and extension controls; release depends on operational readiness; AI and agentic behavior inherit every applicable non-AI requirement. A specialized standard MAY strengthen these requirements but MUST NOT weaken them without an explicit supersession rule.

40. Current External Authority Register

Authority	Relevance	Official Location	Status	Validated
ISO/IEC/IEEE 15288:2023	System life cycle information and processes	https://www.iso.org/standard/81702.html	Published	2026-09-17
ISO/IEC/IEEE 29148:2018	Requirements information items	https://www.iso.org/standard/72089.html	Published	2026-09-17
NIST SP 800-218	Secure Software Development Framework 1.1	https://csrc.nist.gov/pubs/sp/800/218/final	Final 1.1; Rev. 1 draft active	2026-09-17
RFC 2119	Requirements language	https://www.rfc-editor.org/rfc/rfc2119	BCP 14	2026-09-17
RFC 8174	Uppercase requirements language clarification	https://www.rfc-editor.org/rfc/rfc8174	BCP 14	2026-09-17

The authority register is informative unless an adopting organization incorporates a source into a binding obligation. Legal applicability and licensed ISO content must be evaluated by qualified parties. The register records current source identity and relevance without reproducing protected standards text.

41. Control Traceability

Each control MUST remain traceable to:

- the risk or outcome it addresses;
- the applicable profile;
- implementation ownership;
- evidence;
- assessment procedure;
- exceptions;
- external mappings;
- related Foundation controls.

42. Source-Draft Preservation

This enterprise candidate edition preserves every normative control and the substantive source-draft sections. Editorial movement into the enterprise report structure does not remove the original requirement, implementation guidance, evidence, assessment procedure, exception rule, or external mapping.

FOUNDATION STANDARD / STRUCTURAL PART

Part VIII – Appendices

Appendix A – Source-Draft Evolution Notes

- Preserves the source draft's authority classes, documentation map, ADR discipline, runbook structure, traceability, and documentation-as-code requirements.
- Replaces mandatory AI-assistant scripts with a general machine-consumption protocol and explicit trust boundaries.
- Consolidates overlapping repository-layout advice into profile-based requirements.
- Adds assessment procedures, evidence quality, retrieval evaluation, and measurable drift controls.

Appendix B – Change History

Version	Date	Status	Summary
0.2.0	2026-07-18	Working Draft	First standards-program restructuring of the source draft into atomic controls, assurance profiles, evidence, assessment procedures, and cross-standard dependencies.

Appendix C – Control Summary

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-DOC-01	Governance	Documentation authority model	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DOC-02	Metadata	Canonical metadata and identity	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-DOC-03	Discovery	Authoritative documentation map	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-DOC-04	Profiles	Risk-based documentation profile	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-DOC-05	Lifecycle	Status, review, and supersession lifecycle	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-06	Architecture	Architecture documentation and invariants	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DOC-07	Decisions	Architecture and product decision records	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-DOC-08	Contracts	Contract and interface documentation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-09	Traceability	Documentation traceability graph	Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-10	Security and risk	Security, privacy, and risk documentation	Foundational, Advanced, High Assurance	Partial	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-DOC-11	Verification	Test strategy and evidence documentation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-12	Operations	Actionable runbooks and operational documentation	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DOC-13	Release	Release documentation and evidence manifest	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-14	Users	Audience-appropriate user information	Foundational, Advanced, High Assurance	Manual	Material
MYTHOS-FND-DOC-15	Automation	Documentation-as-code controls	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-DOC-16	Generation	Generated-documentation boundaries	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-DOC-17	Machine consumption	Safe machine and AI consumption	Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-18	Quality	Documentation quality and drift management	Foundational, Advanced, High Assurance	High	Critical

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0002
version: 0.2.0
profile: foundational | advanced | high_assurance
scope: <bounded systems, teams, environments, and processes>
assessment_period: <start/end>
assessor: <person or independent body>
tailoring_decisions: []
exceptions: []
findings_summary:
  satisfied: 0
  partially_satisfied: 0
  not_satisfied: 0
  not_applicable: 0
  not_assessed: 0
residual_risk_owner: <accountable role>
approval: <record reference>
```

Appendix E – Publication Review Checklist

- [ ] Domain technical review completed
- [ ] Security and privacy review completed
- [ ] Current primary sources validated
- [ ] Exact external mappings reviewed
- [ ] All controls testable
- [ ] Evidence requirements sufficient
- [ ] Assessment procedures repeatable
- [ ] Executive findings supported
- [ ] Legal applicability reviewed where required

- [ ] Accessibility and publication quality verified
- [ ] Machine-readable control catalog validated
- [ ] Change and review record complete
- [ ] Formal approval recorded